Information rights report
Quarter 4 2016/17

Contents

1. Important policy issues

EU-US Privacy Shield

Since it became operational on 1 August 2016, the preparations for the implementation and functioning of the Privacy Shield have continued between the EU (both European Commission and the data protection authorities of the Article 29 Working Party) and the US. The preparations included the setting up of the EU Centralised Body (which will be the EU liaison body with the US Ombudsperson as the mechanism responsible for dealing with data subjects' enquiries about the US signals intelligence practices) and the EU Informal Panel (which will provide binding advice to US organisations in relation to unresolved complaints from individuals about the handling of their personal information transferred under the Privacy Shield).

In order to enable the public to understand better their rights under the Privacy Shield and how the two EU bodies will work to address their issues and concerns, rules of procedure have been developed together with individual request forms for both bodies. These documents will be published on the WP29 and ICO's websites.

The Working Party will continue to raise with the US representatives any issues affecting the Privacy Shield and its effective operation. Of recent interest has been the question of the effect of President Trump's Executive Order on the Privacy Shield and following this. The ICO issued a statement that we have no indication that the Order creates a legal change to the protection afforded by the EU-US Privacy Shield.

Next steps: the preparation for the Annual Joint Review of the Shield programme by the Commission, representative DPAs and the US authorities and the conduct of the Review in autumn 2017.

Contact: Geraldine Dersley/Naomi Osborne-Wood

GDPR

<u>Article 29 Working Party guidelines</u>
The ICO led in the Article 29 Working Party drafting European Data Protection Board 'Guidelines for identifying a controller or processor's lead supervisory authority'. Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the cross-border processing of personal data. The guidance addressed important terminology which will set the bar for future assessments on cross border cases under the GDPR, such as how to determine the impact on data subject(s) in each jurisdiction in relation to 'substantially affects' in article 4, and how to determine a data controller's 'main establishment' in a

specific case. The ICO also inputted into the EDPB guidelines on role of a Data Protection Officer which were also amended, like the 'Lead Authority' guidelines between December - March then adopted in April 2017.

Contact: Gemma Farmer

Data portability guidelines

http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Article 20 of the General Data Protection Regulation introduces the data subject's right to data portability, under certain conditions, to receive the data he has provided to a controller and to transfer data to and into another, without being prevented from doing so by the controller. The Guidelines on Data Portability were first published in December 2016 and opened for comment from external stakeholders. The comment period closed in February 2017 and the final version of the guidelines were adopted. The ICO was part of the drafting team.

Guidelines on Data Protection Impact Assessment

http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Article 35 of the General Data Protection Regulation introduces DPIAs in order for a data controller to take account of the data protection risks in particular data processing operations. The Guidelines on Data Protection Impact Assessment were published for comment from external stakeholders. The ICO participated in the drafting team.

Contact: Simon Rice

The ICO is also currently taking the lead in the Article 29 Working Party on guidelines addressing the concept of profiling and led the relevant session on this topic at the second ever Article 29 Working Party stakeholder consultation known as 'Fablab' which serves to ensure that the Working Party is starting to fulfil its obligations under article 70, (4) GDPR, to ensure that 'the Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period.' Another Fablab is likely to be held later in 2017 on international transfers and transparency issues under GDPR.

We are also co-rapporteur for the EDPB guidelines on consent and certification.

Next steps: The completion of EDPB guidelines on profiling and consent is expected for Q1 2017-18. Guidelines on transparency issues, data breach notification and certification, as well as the GDPR aspects of international transfers are expected later in 2017.

Contact: Gemma Farmer/Carl Wiper/ Hannah McCausland/Simon Rice/Lynsey Smith

ICO GDPR guidance

Profiling
We have published an ICO consultation document on the subject of profiling to inform the content of the EPDB guidelines.

Contact: Karen Harris/Carl Wiper

Consent
The ICO published our first topic specific piece of GDPR guidance on consent for publication. We have received 300 responses which we are currently analysing and feeding into the guidance in order to finalise it. We are also using this to contribute to the European guidelines on consent mentioned above.

Contact: Jo Crowley/Lynsey Smith

Big data, artificial intelligence, machine learning and data protection
We published our paper containing practical advice on the tools that can assist organisations with compliance when using big data analytics, artificial intelligence and machine learning was published in March 2017. It included specific content regarding privacy impact assessments and also touched on the implications from a GDPR perspective.

Contact: Alex Hubbard/Carl Wiper

E Privacy Regulation
We blogged about the e-privacy reform, explaining that there has been a proposal for an e-privacy regulation and setting out what to expect in the coming months. To date we have provided our views to those drafting the proposal and have contributed to the Article 29 Working Party Opinion 01/2017 on proposed ePrivacy Regulation (2002/58/EC), http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

Next steps: We are likely to have a role in providing expert advice to assist the UK government during this process. We also plan to produce an initial guidance document setting out the key issues arising from the reform later in the year.

Contact: Lynsey Smith/Simon Rice/Peter Brown

Data Protection Act 1998 Guidance
Draft guidance on Privacy Enhancing Technologies and organisations' use of passwords for online authentication have been prepared and moved for technical and policy review. It is hoped these will be published during Q1 2017/18. A deeper dive into the processing of personal data by new consumer products and services and a comparison with the privacy

information provided to consumers is also progressing, to be finalised during 2017.

Contact: Simon Rice/Peter Brown

Subject access and disproportionate effort
We have reflected on the key judgments in the cases of Dawson-Damer and Ittihadieh which addressed the concept of disproportionate effort in relation to subject access requests. Amendments to the SAR code have been drafted as well as associated internal products to communicate our policy position for staff. We hope to publish these in Q1 2017/18

Contact: Viv Adams

International engagement

Common Thread Network (CTN) – data protection authorities across the Commonwealth
The CTN common statement on the occasion of the International Data Protection Day (28 January 2017) was published on the CTN website. This confirmed how members of the Network, including the ICO, are united in pursuing greater cooperation. It also defined the ability of ICO and other CTN members to adequately deliver and promote data protection to UK and other nationals across the Commonwealth.
ICO outreach to Commonwealth countries continued with ICO Head of International Strategy and Intelligence participating in the CTO Commonwealth Cybersecurity Forum in London on 22 March 2017. His panel specifically discussed privacy and data protection issues in the Commonwealth and proved a great opportunity to present ICO's views and update on the implementation of the European Data Protection Reform to new audiences. The CTN is co-chaired by the UK ICO and the Canadian Office of the Privacy Commissioner.

Next steps: ICO Head of Enforcement will be attending the second Data Protection Conference in Ghana on 20-21 April 2017 to meet with potential partner African data protection regulatory agencies to discuss the benefits of the Network. As co-chair of the CTN, ICO will also report back to members on the significant progress made during the period. The Common Thread Network will aim to further increase membership across the Commonwealth and engage with the Commonwealth Secretariat exploring potential areas of common work. The ICO will assess the CTN contribution to the ICO's new International Strategy.

Contact: Alain Kapper

Centre for Information Policy Leadership
We presented our views on Transparency under the GDPR and took part in a panel at the CIPL event in Madrid. We also provided an update on the UK implementation progress, including within the ICO.

Contact: Jo Pedder

Government of the Philippines
The ICO held a teleconference with representatives of the World Bank and the Government of the Philippines and their National Archives. The ICO provided insight and advice about the implementation of Freedom of Information legislation based on our own experience.

Contact: Jo Pedder

Technology
We delivered Know About sessions for ICO staff on Tor and the Dark Web in order to ensure staff remain up to date with emerging technologies. A trial of Wi-Fi analytics software was also conducted in order to gain a deeper understanding of the current state of the technology following the publication of guidance in 2016. A review of video redaction software was also conducted in order to inform policy areas.

Contact: Simon Rice

Digital Economy Bill: data sharing and age verification

The Digital Economy Bill has completed its passage through Parliament as part of the wash up of legislation before the general election and is expected to receive Royal Assent shortly. A large number of amendments were tabled in the Lords, including provisions for ICO fee-raising powers and improvements to the data sharing and age verification arrangements.

The Commissioner in her evidence to the Commons Bill Committee called for strengthened safeguards on data sharing and recommended providing references to the ICO's codes on privacy impact assessments and privacy notices on the face of the Bill. We have held detailed discussions with the Cabinet Office and DCMS on amendments to achieve this and submitted briefings to interested Lords to provide updates on progress and our views on the provisions of the Bill.

Outcome: The government tabled amendments to the Bill in the Lords which referenced the ICO's PIA and privacy notices codes, as well as fee-raising powers for the ICO. There were a large number of amendments to Part 5 of the Bill concerning data sharing but most of these were tabled by the government and have led to improvements in terms of safeguards and Parliamentary scrutiny. Due to interest in our views on the Bill, we

produced two briefing notes for the Lords at Report Stage that were referred to by a number of front bench peers during the debates and appear to have been influential in gaining cross-party support for data sharing provisions, accompanied by strengthened safeguards.

Future work: We shall continue to engage with the Cabinet Office and DCMS as they develop proposals arising from the Digital Economy legislation. We shall respond formally to any consultations on the data sharing codes which are likely to be launched after the general election. We will remain alert to civil society concerns over the data sharing proposals as they are developed.

Contact: Judith Jones, Jonathan Bamford

Political parties and electoral issues

The snap general election has brought forward our plans to improve political parties' data protection compliance, as well as increased our ongoing engagement with the Electoral Commission, particularly on our respective reviews into the use of data analytics by political parties. The Commissioner has written to all the main UK political parties reminding them to comply with data protection and electronic marketing rules when campaigning during the general election. They will also be signposted to our new updated political campaigning guidance. The ICO will also be offering a meeting on 4 May with the main political parties to discuss data protection and PECR obligations and any issues arising from the updated guidance.

Outcome: An event for political parties has been arranged for 4 May 2017, where we shall explain how the updated guidance will cover issues such as the use of data analytics and associated technologies and will reflect our latest advice on marketing and consent, emphasising the need to be transparent when processing citizens' data. The update will pull together advice provided elsewhere to help political parties comply with the law and maintain citizens' trust and confidence in the democratic process.

Future work: We shall monitor the parties' campaigning practices during the general election. We shall also remain alert to any complaints received during the election and work with the House Authorities if any issues arise relating to personal data of constituents held by departing MPs.

Contact: Jonathan Bamford, Judith Jones, Jenny Childs

REDACTED

TPP SystmOne sharing of patient records

We have engaged heavily with NHS Digital and TPP for some time in relation to our concerns regarding their SystmOne data sharing program. We wrote to TPP in June to advise them that we had concerns regarding the way in which the system complied with principles 1 and 7 of the DPA. We have continued to engage on the matter since then and in February of this year, we called a meeting involving representatives from the various interested parties. TPP, NHS England, NHS Digital, the British Medical Association and the Royal College of General Practitioners were all present. At the meeting NHS Digital and TPP discussed the initial steps they were taking to make changes to SystmOne.

We continue to have meetings and discussions with NHS Digital and TPP and they are well aware of our main compliance concerns.

Outcome: There has been some progress towards making some fixes to the way in which TPP operates. However, there is still significant work to be done to address our major concerns with the way in which SystmOne operates.

Future work: We continue to engage with NHS Digital and TPP, as well as others, about concerns relating to SystmOne. There is also a plan to hold another meeting in May or June, again with representatives from the various interested parties present, where progress to date can be discussed.

Contact: Ian Inman, Andrew Rose

National Data Guardian (NDG) Consent Review

The Secretary of State for Health commissioned the NDG to review and produce a report detailing whether the NHS should offer an opt out of data being used for purposes other than direct care. We were asked to take part in the review panel.

The NDG has now published her report into data security standards and consent.

Outcome: We were involved in discussions with the NDG prior to the publication of her report. We discussed a number of the recommendations in the report with her in some detail. In particular we raised some concerns about the status that had been given to some of the ICO guidance in the report, particularly the Anonymisation Code of Practice. In its draft form the report seemed to suggest that the Anonymisation Code

was more like a statutory code that organisations must comply with and that there could be serious consequences.

We have responded to the Department for Health Consultation that followed up the publication of the report. We have also been asked to sit on the advisory group looking into how the consent model should be implemented.

Future work: We will be making sure we are present at the meetings of the advisory group and we are also working with NHS Digital on the redesign of the IG Toolkit which is looking to implement the new security standards.

Contact: Stacey Egerton, Victoria Cetinkaya

Pseudonymisation and anonymisation

There has been significant work undertaken on this over the last 12 months within the health sector. There have been various attempts at drafting an anonymisation standard to improve the ability to share data within the health and social care sectors. This issue is also central to how the opt out model will work under the recommendations set out by the NDG review.

This matter has been complicated by the inclusion under the GDPR of pseudonymised data and the fact that, in some contexts, pseudonymised data will not be 'anonymised'. We have raised this issue with NHS England and we are continuing to work with them and others in the health sector to address concerns.

Outcome: We have made our policy position on this matter clear to both the Department for Health and NHS England.

Contact: Ian Inman

REDACTED

REDACTED

REDACTED

Freedom of Information- Police Federation

We have provided advice on implementation, and an introductory workshop for senior staff of the Police Federation, prior to it being added

to Schedule 1 of FOIA as a public authority for the purposes of the Act with effect from early April 2017.

Outcome:
We have helped build competence within the Police Federation in advance of their new obligations to ensure they are equipped to discharge these.

Future work: There will be ongoing engagement to ensure that the new obligations are complied with in practice.

Contact – Steven Dickinson

REDACTED

REDACTED

2. Data breaches and other high profile cases

Enforcement

REDACTED

In Q4 it was widely publicised that services provided to the NHS by Capita had broken down, resulting in a backlog of medical documents waiting to be delivered between different medical services. A similar problem, which was not widely reported, existed with another company providing services to the NHS SBS Services. The ICO was aware of the situation and was investigating the cause of the problem and the intended remedial action.

REDACTED

Until recently all cyber crime incidents reported to the ICO were investigated by non-sector specific case officers. However, as the number and complexity of cyber crime incidents reported have increased it became apparent that this approach was no longer sustainable. Therefore, at the start of Q4 we restructured our civil enforcement team and created a team dedicated to investigating cyber related incidents.

The cyber crime sector team is manned by case officers with the required ITC skills to be able to deal with current and emerging threats in the cyber crime arena. A number of high profile cases are currently under investigation.

We are liaising with law enforcement agencies and other regulators to ensure we have an organised approach, sharing information where appropriate.

3. Ongoing investigations

Enforcement

Investigations

The ongoing criminal investigations into data thefts relating to the auto-body repair industry continue (Operations Pelham and Huron). During Q4 we executed a search warrant in relation to Huron during which we seized a number of items for forensic examination. Further search warrants in relation to Operation Pelham are planned for Q1 2017/18.

4. Enforcement action

PECR

This quarter we issued nine civil monetary penalties totaling £803,000 for contraventions of the Privacy and Electronic Communication Regulations (PECR), by organisations making or sending unsolicited marketing calls and messages. The largest penalty was £270,000 against Road Traffic Consult t/a Media Tactics for mass volume unsolicited automated marketing calls.

Other fines included ones issued against LAD Media Limited for £50,000, Digitonomy Limited for £120,000, IT Protect Limited for £40,000, PRS Media Limited for £140,000, Munee Hut LLP for £20,000, Honda (Europe) Limited for £13,000 and Flybe for £70,000; the latter two cases for unsolicited email marketing.

For the full year, this resulted in our strongest performance ever with 23 monetary penalties being issued for marketing contraventions totalling £1,923,000.

This quarter we also served an Enforcement Notice to accompany a civil monetary penalty of £80,000 issued against Xternal Property Solutions Limited. And one Preliminary Enforcement Notices was issued against an organisation in this period.

In January 2017, the ICO assumed statutory responsibility from Ofcom for the Telephone Preference Service (TPS). Monthly contract management meetings have been reestablished with the concessionaire, and integration of management information and reporting is underway. We are developing closer co-operation between TPS staff and the ICO's intelligence and enforcement teams.

In Q4, complaints to the Telephone Preference Service were 18,607, compared to 23,058 in the same quarter last year. A reduction this year of 19%.

We issued two fixed penalty notices under PECR against communications service providers for failing to report an unauthorised disclosure of personal data as a result of a security breach. Vodafone and EE both discharged their liability by paying £800 on receipt of the Notices of Intent.

We monitored five organisations this quarter which we believe represent risks in relation to compliance with PECR. We held eleven meetings with organisations to tell them to improve their direct marketing practices. In

the year to date, we have monitored 18 organisations and held 31 compliance meetings.

DPA

We issued five civil monetary penalties in Q4 relating to breaches of data protection principles, bringing the annual total to 16 with a total value of £1,624,500.

Q4 also saw the conclusion of a record intake of cases for the Civil Investigation Team, with over 2,500 cases being created in the year. The continuing success of the triage and risk assessment process saw the allocation of a notable volume of low risk incidents to the wider Operations Directorate. Further streamlining of the triage process has brought about significant reductions in the number and age profile of cases awaiting allocation, although allocated caseloads in the main remain high with a total caseload of 437 cases carried forward from Q4 to Q1 2017/18.

REDACTED

All civil monetary penalties notices relating to P7 breaches have been paid

In Q4 we prosecuted five criminal cases, three s55 cases involving the unlawful obtaining or disclosing of data, and two s47 cases relating to enforcement notices. Fines and costs amounted to over £4k.

One case involved a serious breach of patient records in a hospital where over 3,000 records were accessed over a 26 month period without lawful excuse. Those affected included colleagues of the offender and whilst there was no personal gain for the individual, nor evidence that any information had been disclosed or passed on, this was nevertheless a serious breach of trust and attracted significant media coverage.

In all five criminal cases the defendants pleaded guilty at the earliest opportunity. In addition we issued a caution for a further s55 offence where CCTV footage had been inappropriately uploaded onto a social media platform.

REDACTED

Technology Team input

Technology team expertise was provided to ongoing enforcement activity including to high profile cyber-attacks and strategic casework. A series of meetings were also undertaken to provide mentoring to specialist

technical Investigators recently recruited into the Civil Investigations Department.

Contact: Simon Rice

5. Consultations

Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions
The ICO has responded to the joint European Supervisory Authorities' discussion paper on the use of big data by financial institutions. The European Supervisory Authorities, or ESAs, are the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority.

The paper presented a thorough assessment of the potential benefits and risks linked to the use of Big Data by financial institutions and requested feedback comments in order to better understand the phenomenon and decide what regulatory and supervisory action may be required.

The ICO's response, which also benefitted from the input of partner European Data Protection Authorities in the Article 29 Working Party, highlighted that data protection, far from being a barrier to big data, can help encourage innovation and serve as the foundations on which successful big data projects can be built. Data protection is a framework for fair, responsible and appropriate processing in a big data context and compliance with data protection legislation, notably through tools and solutions embedding data protection at the outset a big data project (like DPIAs, Privacy by design, algorithmic auditing) will be a key factor in helping organisations addressing the various privacy risks identified by the ESAs.

Contact: Alain Kapper/Alex Hubbard

Unlocking the UKs High Tech Economy – Consultation on the safe use of drones in the UK

House of Commons Science and Technology Committee – inquiry into algorithmic decision making

6. Other

Performance Improvement Department

The final quarter of the year has again been a productive one for the Performance Improvement Teams. Intake this year has been the highest on record, and we haven't been able to close everything that we've received. That isn't surprising because the numbers in have been unprecedented. We received over 18,000 data protection cases this year, and just under 5,500 freedom of information ones. The profile of information rights is high and will only get more prominent over the next 12 months and beyond.

In terms of the departments overall output it has been a record breaking year. In total over 22,500 information rights cases have been handled and dealt with 17,359 completed data protection complaints versus 15,718 last year. That is a productivity increase of over 10 percent. We have also dealt with more freedom of information cases than last year, 5,177 against 5,068 from 2015/16 and around 250 appeals to the tribunal. We've also looked at another 770 self-reported incidents. We don't have any cases over a year old on the books, and are likely to have achieved 90% of our case closures within three months for data protection and 6 months for freedom of information.

More detailed statistical information is included with other papers for Management Board, however everyone in the department is aware that our output isn't about delivering impressive casework statistics, it's been about helping people, and this year we have been involved in helping loads of them.

Freedom of information monitoring activity has continued. In March we raised the threshold that triggers the ICO's monitoring of public authorities when responding to freedom of information requests. Public authorities will now be considered for monitoring if fewer than 90% of their freedom of information responses fall within the statutory timescale.

Andy Laing
Head of Performance Improvement.

ICO training

495 hours of training on information rights was delivered to 298 ICO delegates during the year across all the information rights legislation regulated by the ICO. 31 delegates successfully obtained the BCS data protection qualification. The e-learning module on the GDPR continues to be completed by staff across the ICO.

Contact: Lisa Atkinson

International Transfers Workshop

As part of its preparations for the application of the GDPR, the ICO held a workshop on the topic of international transfers in London on 25 January 2017 with Bruno Gencarelli from the European Commission as a guest speaker. The aim of the workshop was to engage with key stakeholders in the area of international transfers, including organisations representing business and industry, specialist law firms and large multinational data controllers which may have their main establishment in the UK; to provide stakeholders with an indication of the ICO's views on the international transfer mechanisms set out in the GDPR and to listen to stakeholders' questions and views on the principles which underpin those mechanisms, as well as on how they think the measures will work in practice. Outcomes from the workshop will now feed into the GDPR International Transfers project.

Contact – Anulka Clarke/Michele Voznick

DRIPA audits

The Communications Audit team have completed audits with all UK-based Communications Service Providers (CSPs) who are currently subject to a Data Retention Notice, under the Data Retention Regulations 2014 and Data Retention and Investigatory Powers Act 2014 (DRIPA). An End of Year Report has been drafted to outline key themes that emerged from the audits and to highlight some over-arching issues that the team have identified in the course of their work. The current intention is for this report to be shared with the Home Office, the Interception of Communications Commissioner (IoCCO) and the CSPs; consideration will also be given to publishing a suitably redacted version.

Contact – Liam Duncan

Central government breach reporting

Following the NAO report which highlighted concerns about breach reporting arrangements within central government departments the first six information risk reviews (IRRs) of government departments were completed by Good Practice. A further six visits are scheduled for Q1 2017/18, with plans in progress for the remaining four departments. Common themes are already emerging from the findings and a full report will be published once all visits have been completed.

Contact – Vicki Heath

Local government breach reporting

Project Haraz is a collaboration between Enforcement and Good Practice; initially 15 local authorities were identified to be potentially under-reporting breaches based on their size and geographical location. From our initial approach, six desk-based Information Risk Reviews (IRRs) have been completed, with dates for another three to be confirmed. Enforcement have had no response from four of the identified councils and a further two have refused the offer of an IRR. We intend to review the data once all the IRRs are complete to look for any emerging patterns and trends.

Contact – Cath Halaas

Audit outcomes reporting

During 2016/17 the health audit team within Good Practice identified a trend of poor records management across several health organisations. Based on the audit findings, barriers to complying with the law were identified, which helped us to understand who we needed to educate, and around which issues. A communication plan was then devised to promote the key messages to the target audiences. The result was the publication of a range of online resources in March 2017. Some were targeted to directly educate information governance specialists, while others equipped those specialists to educate colleagues within their organisation. Feedback has been positive and the analytics show the initiative is already proving popular. Based on the success of this project, a follow up is now being planned around promoting the assessment of the legality, benefits and risks of data sharing in the health sector by organisations; with plans to use similar outcomes reporting across other sectors during 2017/18.

Contact – Leanne Doherty